Homeland Security Advanced Research Projects Agency

Cyber Security Division

Trustworthy Cyberspace: Leveraging SwA initiatives to implement the Strategic Plan for the Federal Cybersecurity R&D Program

Douglas Maughan, Ph.D.

Division Director

March 28, 2012

Homeland Security

Science and Technology

Comprehensive National Cybersecurity Initiative (CNCI)

Focus Area 1 — Establish a front line of defense

- Reduce the Number of Trusted Internet Connections
- Deploy Passive Sensors Across Federal Systems
- Pursue Deployment of Automated Defense Systems
- Coordinate and Redirect R&D Efforts

Focus Area 2 — Resolve to secure cyberspace / set conditions for long-term success

- Connect Current Centers to Enhance Situational Awareness
- Develop Gov't-wide Counterintelligence Plan for Cyber
- Increase Security of the Classified Networks
- Expand Education

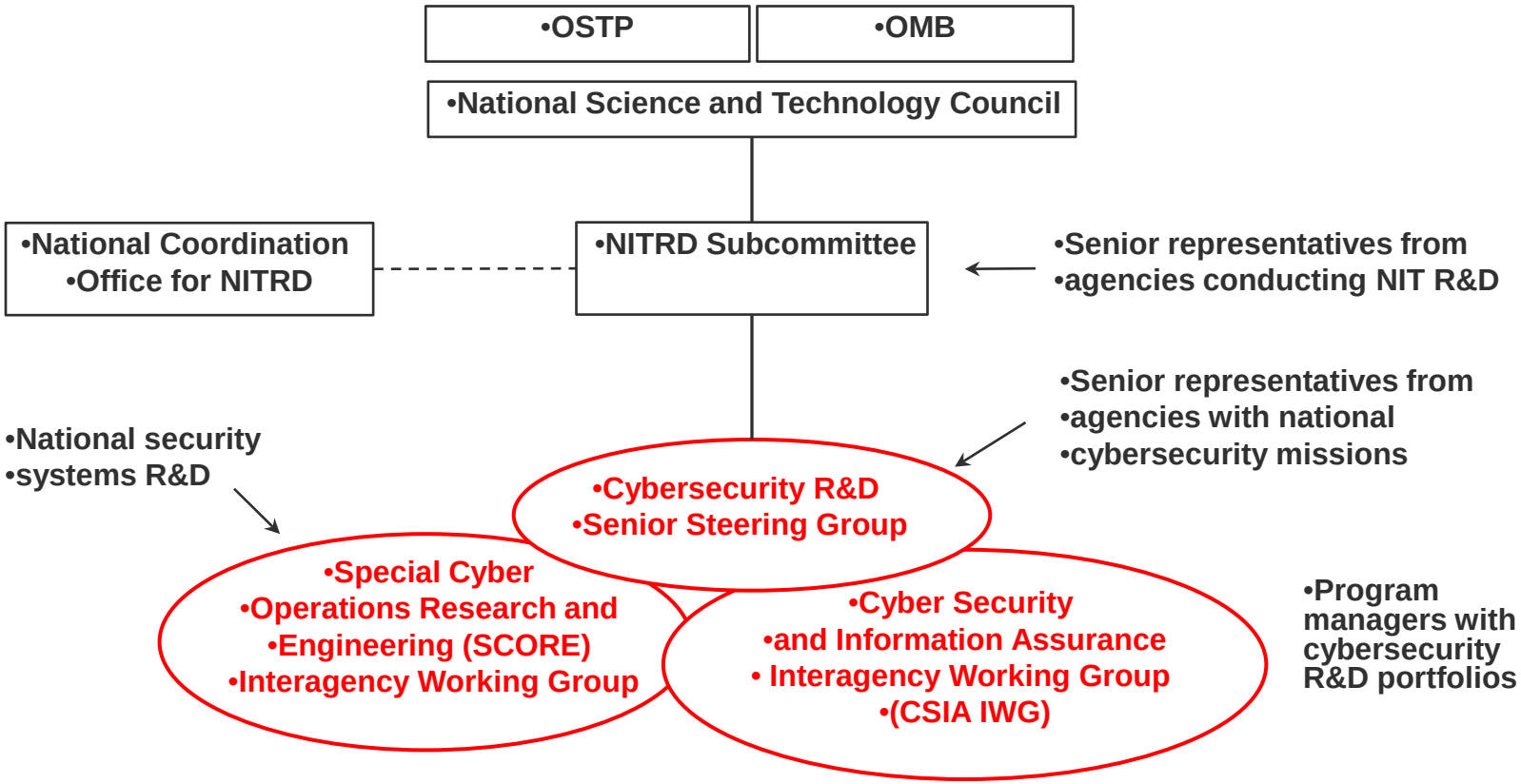
Focus Area 3 — Shape future environment / secure U.S. advantage / address new threats

- Define and Develop Enduring Leap Ahead Technologies, Strategies & Programs
- Define and Develop Enduring Deterrence Strategies & Programs
- Manage Global Supply Chain Risk
- Cyber Security in Critical Infrastructure Domains

Homeland Security
Science and Technology

http://cybersecurity.whitehouse.gov

NITRD Structure for Cybersecurity R&D Coordination



Homeland Security
Science and Technology

Federal Cybersecurity Research and Development Program: Strategic Plan

Federal Cybersecurity R&D Strategic Plan

- Research Themes
  - Tailored Trustworthy Spaces
  - Moving Target Defense
  - Cyber Economics and Incentives
  - Designed-In Security (New for FY12)
- Science of Cyber Security
- Transition to Practice
  - Technology Discovery
  - Test & Evaluation / Experimental Deployment
  - Transition / Adoption / Commercialization
- Support for National Priorities
  - Health IT, Smart Grid, NSTIC (Trusted Identity), NICE (Education), Financial Services

Released Dec 6, 2011

http://www.whitehouse.gov/blog/2011/12/06/federal-cybersecurity-rd-strategic-plan-released

Homeland Security
Science and Technology

Federal Investments across All R&D

- Big Data
- Cloud Computing
- Cyber-Physical Systems
- Healthcare IT
- High End Computing
- Software Design and Productivity
- STEM Education

Homeland Security
Science and Technology

And there's more…

•Lots of Bad Code

"

•More than **98% of PCs** have one or more **vulnerable** programs.

•http://secunia.com/blog/56/

•Tools Exist Today

"

•…everybody should be using static analysis tools today. And if you are not using them, then basically you are **negligent**, and you should prepare to be sued by the army of lawyers that have already hit the beach.

• Cigital's CTO Gary McGraw

•No Tool is Perfect

"

•No tool stands out as an **uber-tool**. Each has its strengths and weaknesses.

•Kris Britton, Technical Director
NSA's Center for Assured Software

•Different Semantics

"

•…working with different tool vendors is a confusing and **challenging** and time-consuming process

•Jim Bird, *Building Real Software*
•http://swreflections.blogspot.com/2009_04_01_archive.html

•Sizable Data Sets

Tools generate a lot of data. One test data set consistently returned about **50,000 unique vulnerabilities** across three tools.

Homeland Security
Science and Technology

Designed-in Security

- Designing and developing SW systems that are resistant to attacks
  - Require verifiable assurance about system's attack-resistance to be natively part of the SW design, development, and evolution lifecycle
- Generating assurance artifacts to attest to the system's capabilities to withstand attacks
  - Enable reasoning about a diversity of quality attributes (security, safety, reliability, etc.) and assurance evidence
  - Stimulate further developments in methods and tools for detecting flaws in SW

Software System Development Today: Assertions without Proof

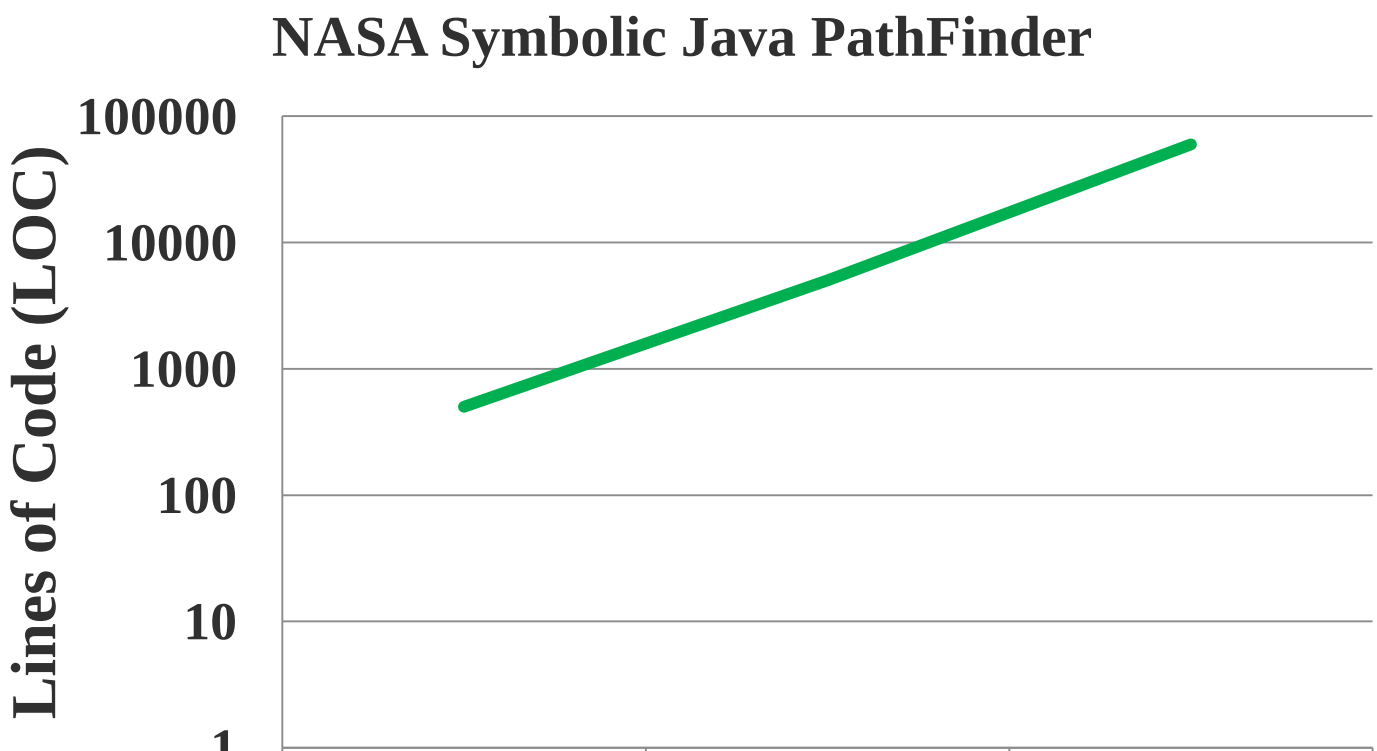
- Programmers are expensive
- Tools are used to economize on programmer time
- Programs grow in pieces from many sources
- Assuring security properties of a system of programs is very difficult

➔ Most programs provide low assurance they are free of security vulnerabilities

➔ Even more significant, most <u>systems</u> of programs are low assurance

➔ High assurance programs don't change very much

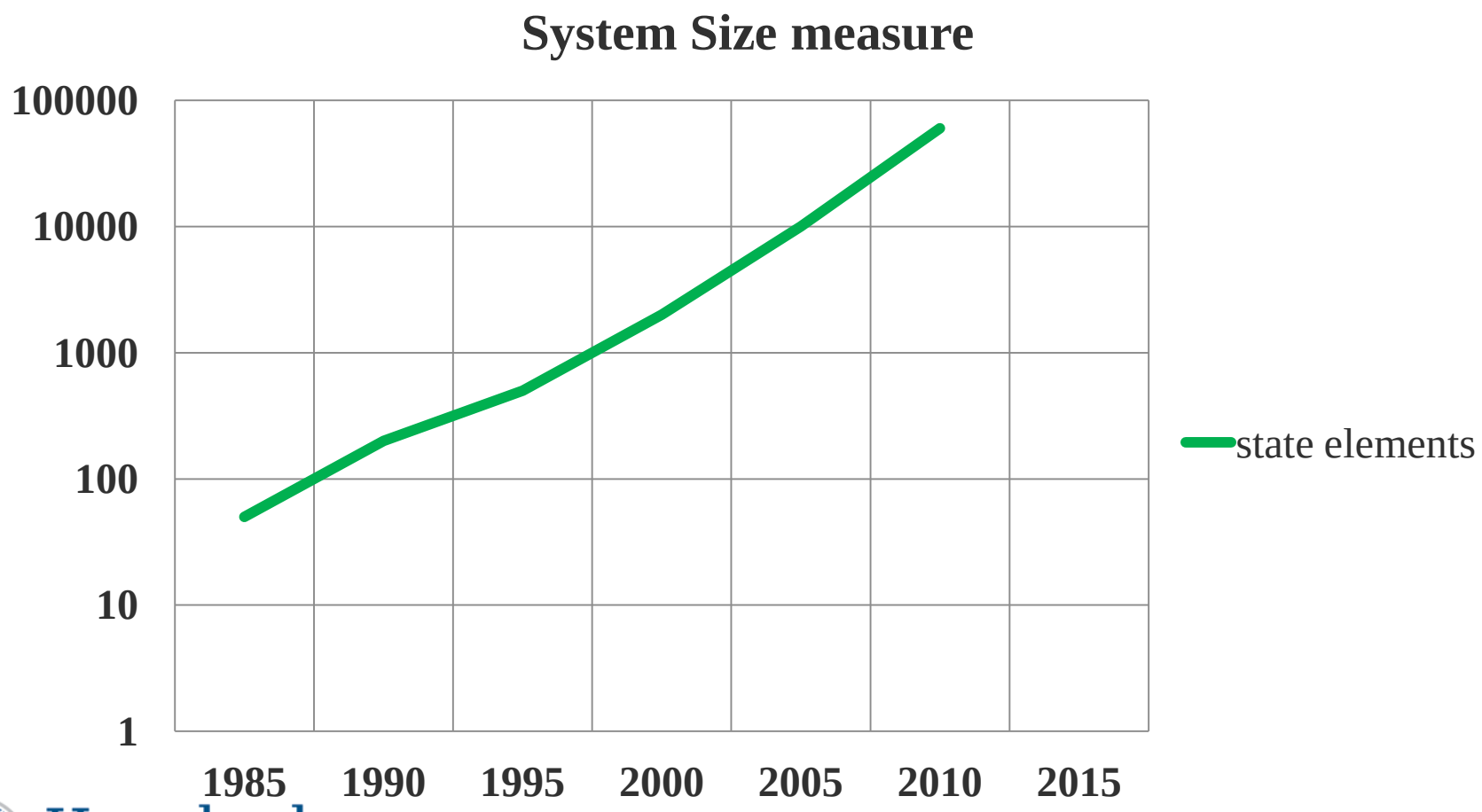
Progress: Dynamic Analysis



	2002	2008	2010
LOC	500	5000	60000

Homeland Security
Science and Technology

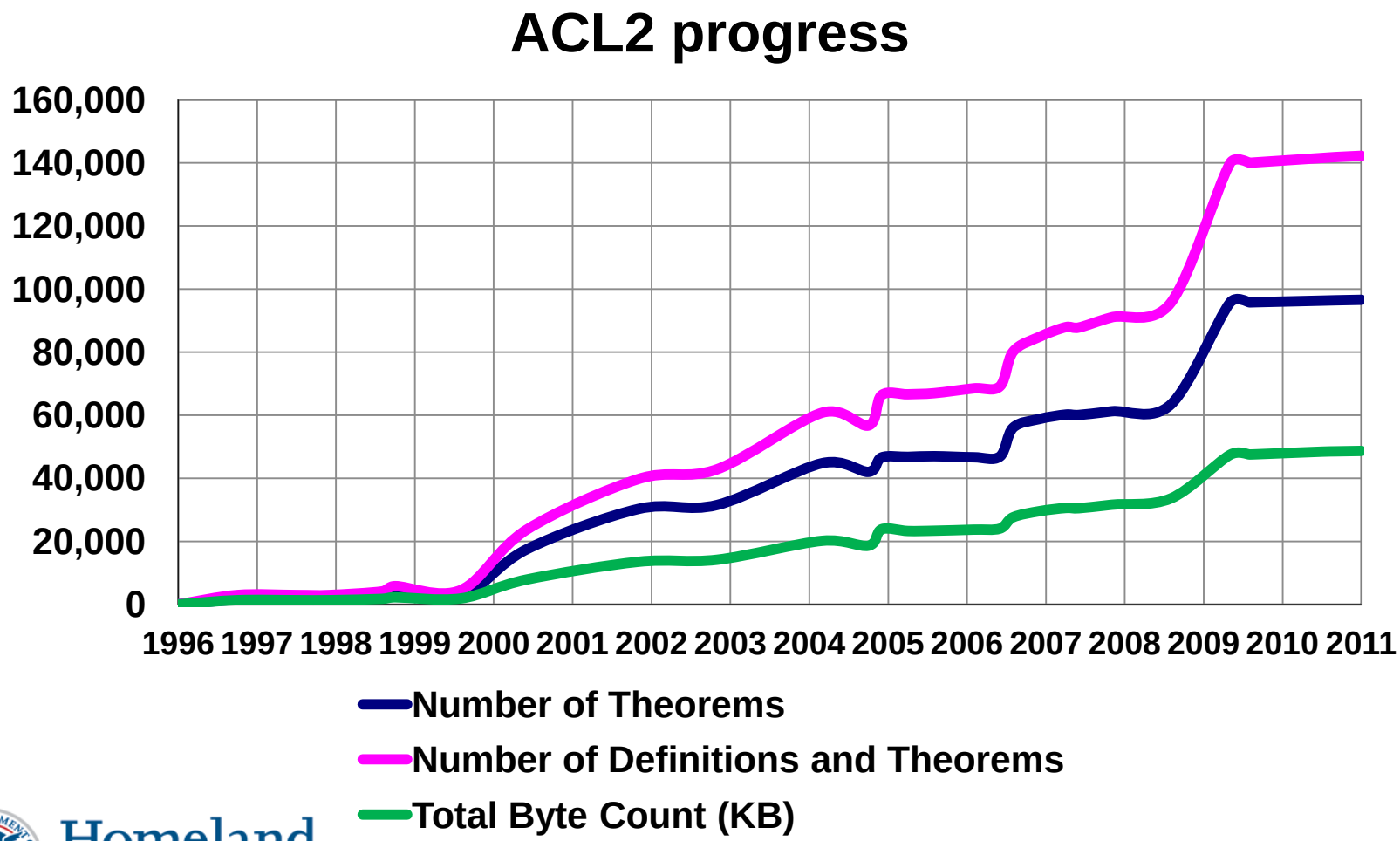
Progress: Model Checking



- Numbers by Jason Baumgartner at IBM Austin

Homeland Security
Science and Technology

Progress: Theorem Proving



- Numbers by J Moore, Matt Kaufmann, Warren Hunt, UT Austin

Homeland Security
Science and Technology

What is needed to bring these advances to bear on system security?

Tools that

- Generate assurance evidence as a system is built
- Can be easily understood and used by real programmers (and yield benefits they can see)
- Can support integration of evidence about various components
- Can be re-applied easily as systems evolve and adapt

Homeland Security
Science and Technology

Some Designed-In Security Research Challenges

- Mathematically sound techniques to support combination of models and composition of results from separate components
- Analysis techniques to enable traceable linking among diverse models and code
- Language design, processing, and tools that can provide high assurance for modular, flexible systems
- Team and supply chain practices to facilitate composition of assurance in the supply chain
- Tools to support assurance evidence management
- Learning what incentives (e.g. ability to quantify results) might motivate the use of these tools

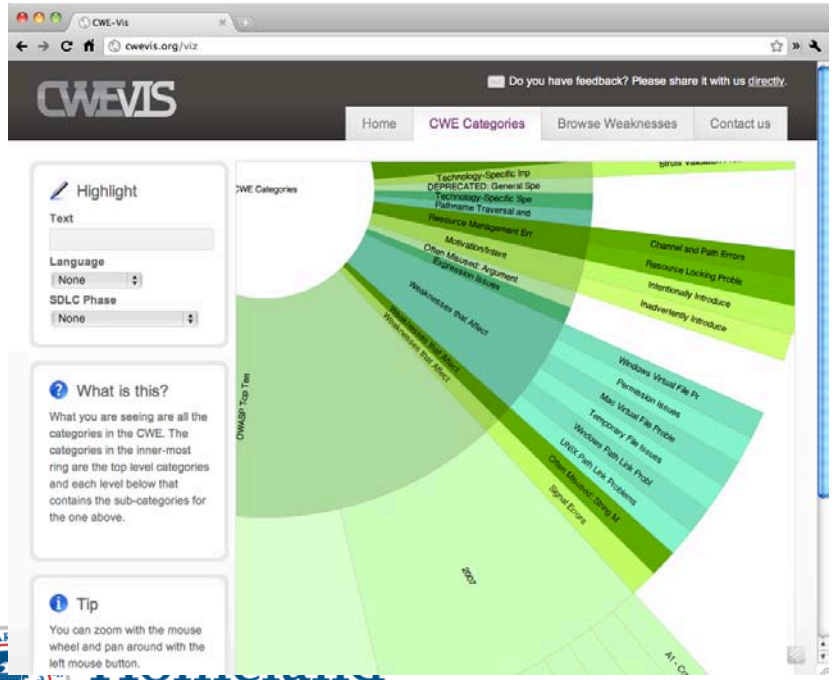
Agency Program Activities

- DHS S&T
- ONR
- IARPA
- NSF

Homeland Security
Science and Technology

Applied Vision

- Open source tool that helps users familiarize themselves with the Common Weakness Enumeration (CWE) through visual means.
- CWE is an international standard created to define a dictionary of software weaknesses.



•CWE-Vis allows the user to:
- •Explore categories
- •Pan and zoom
- •Browse weaknesses

CWEVIS

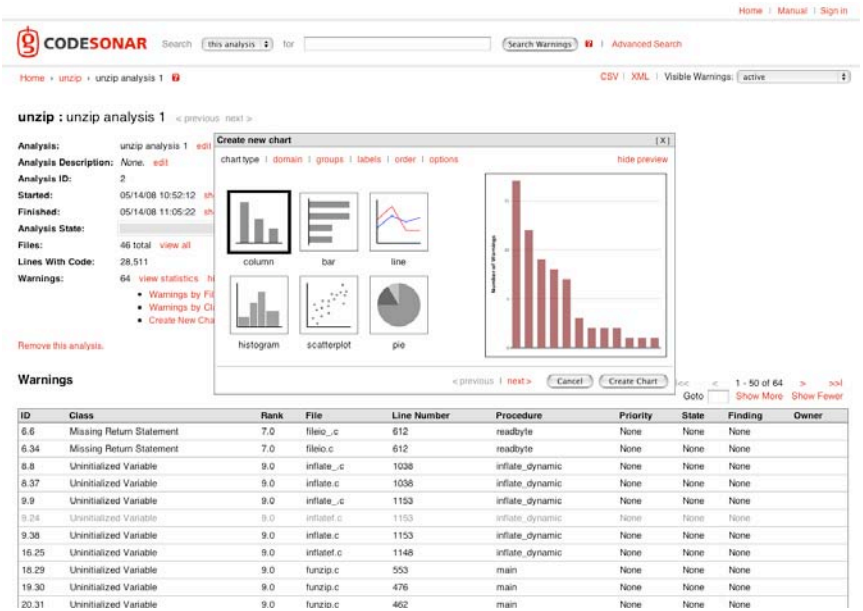
Homeland Security
Science and Technology

Grammatech

- A source-code analyzer that finds serious flaws in software
- Low false-positive rate
  - At cost of missing some flaws
- Easy to invoke analysis
  - No source-code annotations necessary
  - Piggybacks on existing systems
- Easy to interpret results
  - Results hosted in a rich web application

GRAMMATECH

CODESONAR



Homeland Security
Science and Technology

Data Access Technologies

•SwA-Vis

•**S**oftw**a**re **A**ssurance **Vis**ual Analysis

KDM Analytics™

•Tool Output Integration Framework

•An application that brings together **disparate** SwA analysis runs and …

- … normalizes the results in a standard format
- … removes overlapping results
- … visualizes and prioritizes key trouble spots by severity and frequency
- … uses code context to assess the impact of those results
- … filters and highlights based on weakness type and software class
- … shows who is responsible for weaknesses
- … helps assign repair of weaknesses
- … uncovers trends

•**Coverage** •**Priority** •**Traceability** •**Remediation**

Homeland Security

Science and Technology

SwA-Vis

Home
Projects
Options
Dev Tools
SwA-Vis
version 0.2c - 12/23/2011
JGraphT > Analysis Run 1
Weakness count
418 / 418
Displaying all weaknesses
Filters
Severity
Unspecified
1
3
6
Assigned to 1
Escalated
False Positive
New
Tool
Findbugs
Jlint
PMD
Category
BAD_PRACTICE(Findbugs)
Basic Rules(PMD)
Correctness(Findbugs)
Data flow(Jlint)
Design Rules(PMD)
Inheritance(Jlint)
MALICIOUS_CODE(Findbugs)
Tool Code
Weakness Flow
severity
status
tool
category
code
Weaknesses
Id
Weakness
Severity
Codebase Location
Status
Show 25
Displaying 1 to 25 out of 418 total results
•A workflow tailored to each type of user
•Interactive, powerful filtering
•Quickly and effectively triage large weakness lists
•Visualize thousands of weaknesses in a single view

Applied (& Basic) Science Research Direction

F1 : Hardening Hosts - System

- Robust Autonomic Host (monitoring, self-aware, self-healing, graceful degradation, ex-filtration detection)
- Secure Web, and Web Applications (browser, scripting, etc)
- Secure Software Development Environment (development, verification)
- Data Ex-filtration Awareness

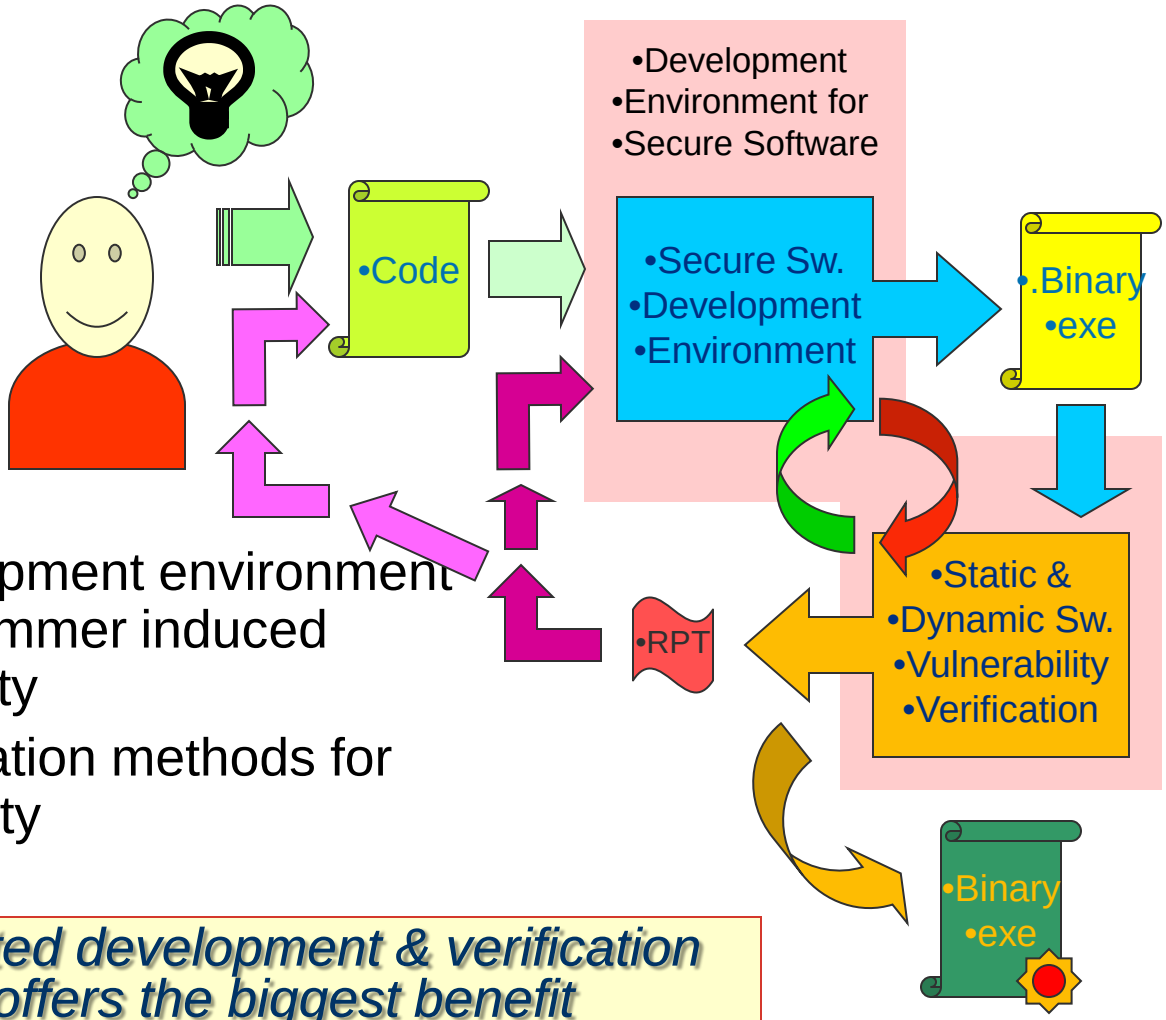
F2 : Hardening data sharing, and integrity (process-process, user-machine, user-process) - Data

- Trust management model and calculus
- Confidentiality in collaboration
- Mobility and Collaboration
- Automatic Crypto Function Generation

F3 : Hardening the Network

- Toward automated dynamic re-configuration (mitigating DDOS)
- Automated network device configuration & policy management
- Enhancing malicious traffic detection, and source tracking

Software Development Environment for Secure System Software & Applications



- <u>Sub-thrusts</u>
- **a.** Software development environment for reducing programmer induced software vulnerability
- **b.** Software verification methods for reducing vulnerability

•Seamless integrated development & verification environment offers the biggest benefit

Science and Technology

Security Aware Software Development Environment

- Security aware software development environment
  - Recognize and identify vulnerability in code
  - Suggest correction for identified vulnerability
  - Generate executable devoid of vulnerability
- Potential approach
  - Security & vulnerability aware compiler
  - High-level design entry, with automated secure code generation
  - High-level design entry, with automatic insertion of security primitive
- Challenge with new development environment
  - Software developer acceptance for new methods, and limitations

Homeland Security
Science and Technology

Software Verification for Reducing Vulnerability

- **Software verification for reducing vulnerability**
  - Security & vulnerability specific verification techniques
  - Identify and isolate potential system vulnerability

Potential approach

- Static (including formal methods)
- Dynamic
- Hybrid

Challenges with the above approaches

- Accuracy & reliability (false positive & false negative)
- Large size & complexity preventing exhaustive evaluation/verification (static, dynamic)
- Continuous evaluation ?, → keep on fixing, when to stop, limits applicability (dynamic)
- Hybrid inherits the strength & weaknesses of both, only less severe in limitations/weaknesses

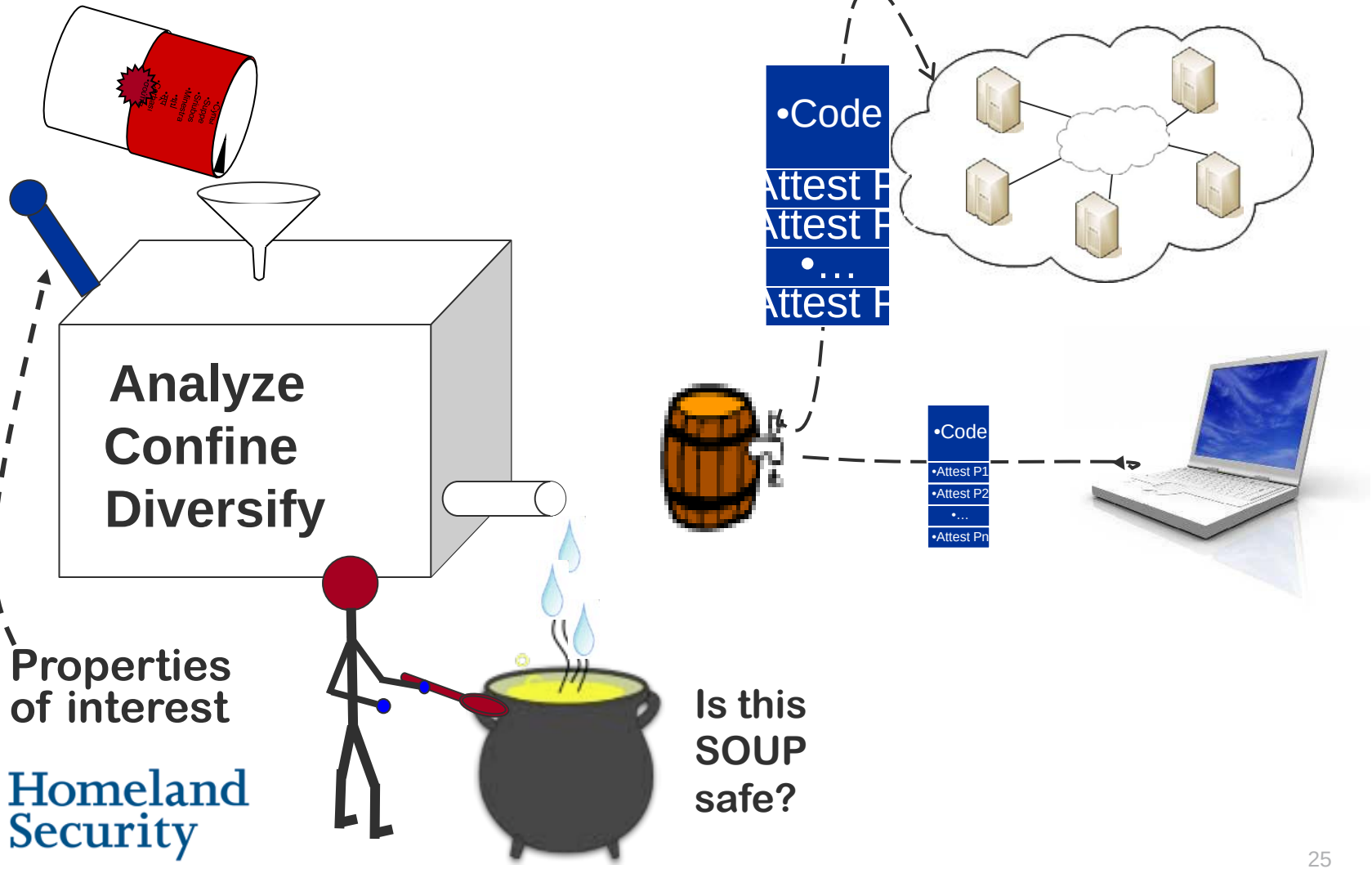
IARPA's STONESOUP

- "Securely Taking on New Executable Software of Uncertain Provenance"
- Develop technology that will allow end users to invoke:
  - advanced automated software analysis techniques to identify vulnerabilities or to assure their absence
  - *tailored confinement* of software execution so that identified weaknesses cannot be exploited
  - *diversification* of software components so residual vulnerabilities will be more difficult for attackers to discover or exploit
- High-risk, high-reward: putting tools in the hand of end-users
  - Opportunity to provide feedback to software vendors

Homeland Security
Science and Technology

STONESOUP Vision

e.g., Binary, C, Java



Homeland Security
Science and Technology

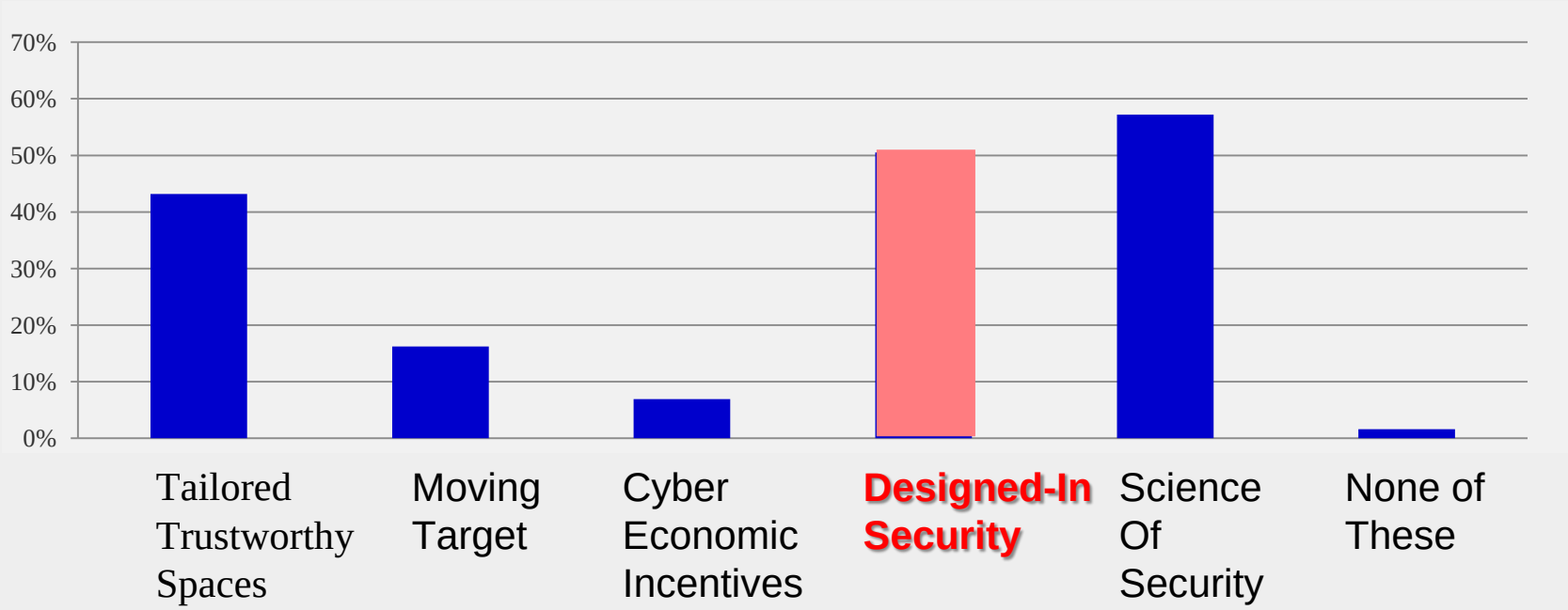
•Where is 'Designed-In Security' Research Focused

- **Survey:** End of fiscal year 2011
- **Awards:** 84 new grants *(71 responded in time for survey)*
- **Overall Distribution:**
  - •3 Large, 18 Medium, 50 Small, 9 CAREER, 2 CRI, 2 CPS
- **Survey Questions:**
  - ✓ Characterize your primary focus in relation to…
    1. The 5 NITRD themes (including "moving target")
    2. Categories based (roughly) on the ISO protocol stack
    3. Categories based on the system development lifecycle
    4. Categories based (roughly) on attack detection / prevention / response
  - ✓ Characterize the results you expect at the *end* of your project
  - ✓ Characterize your project in 5 keywords

Homeland Security
Science and Technology

•NSF 2010 Research Award Outcomes (by theme)

Which of the NITRD-CSIA cybersecurity research themes does your project address? (check all that apply)



•Selected Proposals for 'Designed-In Security'

Principal Investigator	University	Proposal Title
Foster/Walker	Cornell/Princeton	TC: Large: High-Level Language Support for Trustworthy Networks
Zhong Shao	Yale	TC: Medium: Making OS Kernels Crash-Proof by Design and Certification
Clark Barrett	New York University	TC: EAGER: Collaborative Research: Parallel Automated Reasoning
Daniel Bernstein	University of Illinois Chicago	TC: SMALL: Higher-Speed Cryptography
David Brumley	Carnegie-Mellon University	CAREER: Towards Identifying and Eliminating Exploitable Software Bugs
Hao Chen	UC at Davis	TC: SMALL: Designing New Authentication Mechanisms using Hardware…
Yevgeniy Dodis	New York University	TC: SMALL: The Design of Secure Hash Functions and Block Ciphers
Virgil Gligor	Carnegie-Mellon	CNS: EAGER: All Trust is Local: User-Oriented Trust Establishment
Wenke Lee	Georgia Tech	TC: SMALL: A Foundational & Practical Platform for Host Security Applications
Darrell Long	UC at Santa Cruz	TC: SMALL: LockBox: Enabling Users to Keep Data Safe
Jason Nieh	Columbia	TC: SMALL: Improving System Security through Virtual Layered File Systems
Patrick Traynor	Georgia Tech	CAREER: Protecting User Data on Lost, Stolen & Damaged Mobile Phones
Aviel Rubin	Johns Hopkins	TC: LARGE: Self Protecting Electronic Medical Records
Andrew Myers	Cornell	TC: MEDIUM: Higher-level Abstractions for Trustworthy Federated Systems
Patrick Schaumont	Virginia Tech	TC: MEDIUM: Foundations for Future On-chip Fingerprints
Scott Shenker	ICSI UC Berkeley	TC: SMALL: Practical Data Confinement
Roberto Tamassia	Brown	TC: LARGE: Collaborative: Towards Trustworthy Interactions in the Cloud
Jaideep Vaidya	Rutgers	TC: SMALL: Collaborative: Formal Analysis of Access Control Models & Extensions
Moshe Vardi	Rice	CNS: EAGER: Automated Synthesis for System Design

•… Much Remains to be Done to 'Design-in Security'

•…because the problem space is *expanding faster* than we are improving !

- size of software everywhere
- the type and number of interactions with the environment
- increasing variety of platforms and evolutionary diversity

•Usable instrumentation, measurement and assurance evidence

- generate assurance evidence as a system is built and afterwards too!
- support fusing of evidence about various components - *including* tool chains
- re-assess as easily as systems evolve and adapt - *including* continuously certify

Leverage e.g. nature where possible and use society when behavioral

- use physics for built-in security if possible
- adaptive security to broader contexts of norms, culture, privacy, ….

Homeland Security

Science and Technology

Summary

- Cybersecurity research is a key area of innovation needed to support our future
- DHS S&T continues with an aggressive cyber security research agenda
  - Working to solve the cyber security problems of our current (and future) infrastructure and systems
  - Working with academe and industry to improve research tools and datasets
  - Looking at future R&D agendas with the most impact for the nation, including education
- Need to continue strong emphasis on technology transfer and experimental deployments
- Designed-In Security must be a major focus of ALL programs

Homeland Security
Science and Technology

Douglas Maughan, Ph.D.

Division Director

Cyber Security Division

Homeland Security Advanced Research Projects Agency (HSARPA)

douglas.maughan@dhs.gov

202-254-6145 / 202-360-3170

For more information, visit

http://www.cyber.st.dhs.gov

Homeland Security

Science and Technology